UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,138	11/15/2001	Stefan Kemper	10008052-1	6008

7590 08/18/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,138	KEMPER, STEFAN	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on May 23, 2006. Claims 1-20 are currently pending consideration.

Response to Arguments

2. Applicant's arguments filed on May 23, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claims 1, the Applicant argues that the Cited Prior Art (CPA), Henry et al. (U.S. Patent 6,856,800), does not teach the newly added limitations of "allowing continued work on authorized activity" and "denying access to new activities until the authorized activities until the authorized activity is completed." This argument is not found persuasive. The CPA teaches that when a mobile host receives temporary access after local authentication, that a session key with an expiration time is supplied to the host and this session key is used to encrypt and sign packets (column 4 lines 31-53). The continued work on the authorized activity is disclosed by the granting of full access after a remote authentication (column 3 lines 5-33), as once the remote authentication is successful, the mobile host can keep encrypting, signing, and sending packets on the network. The CPA also teaches denying access to new activities until the authorized activities until the authorized activity is completed. The CPA teaches that the mobile host encrypts and signs packets before sending the packets to the

network (column 4 lines 45-50). This encrypting and signing of the packet is interpreted as the authorized activity, and since the packets are not sent without encrypting and signing the packet, the sending of the packets is interpreted as the new activities.

Regarding claims 19-20, the Applicant argues that the CPA does not teach "storing identification data from subsequent user while a previous user's activity is being completed." This argument is not persuasive. The CPA discloses a system where a AAA server is used to authenticate users (column 3 lines 17-32). Furthermore, the CPA discloses that there is a queue where authentication requests are kept until the home AAA can process it (column 1 lines 59-63). This queue wherein authentication information is waiting for processing is interpreted as the storing the identification information while a previous user's activity is being completed. Therefore, it is respectfully asserted that the CPA does teach the limitation of "storing identification data from a subsequent user while a previous user's activity is being completed."

The rejection for the pending claims is maintained below, and applied to the newly added limitations.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1 – 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Henry et al. (U.S. Patent No. 6,856,800).

Regarding claim 1, Henry discloses:

A secure computer device, comprising:

"***means for locally-authenticating a user of the device***" (column 2 lines 12-39, column 3 lines 1-9, column 4 lines 3-24), wherein an access point receives an authentication credential from a network device (secure computer device) and can locally authenticate the user;

"***means for providing granting previously authorized access to the device if the user is locally authenticated***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***means for generating a remote authentication request after a successful local authentication of the user***" (column 3 lines 6-9, column 4 lines 27-30), wherein after the local authentication of the user, the access point forwards the submitted credentials to a remote AAA server, which then performs the entire authentication process;

"***means for granting access to new activities and control parameters on the computer device if remote authentication is successful***" (Figure 4 item 404, column

3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***means for allowing continued work on authorized activity***" where the granting of full access after a remote authentication (column 3 lines 5-33), as once the remote authentication is successful, the mobile host can keep encrypting, signing, and sending packets on the network is interpreted as the authorized activity;

"***means for denying access to new activities until the authorized activity is completed***" wherein the mobile host encrypts and signs packets before sending the packets to the network (column 4 lines 45-50).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Henry discloses:

The device recited in claim 1, further comprising "***means for authorizing the user in response to the successful local authentication***" (column 3 lines 1-9), wherein the access point can locally authenticate a user and then grant temporary access to the user immediately after the successful completion of the local authentication process.

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Henry discloses:

The device recited in claim 2, further comprising "***means for withdrawing the authorization in response to a reply from the server***" (column 3 lines 7-9, column 5 lines 4-17), wherein the remote server determines if the credentials are valid, and if the

credentials are determined to be invalid, a message is sent to the access point which terminates the user's temporary access.

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Henry discloses:

The device recited in claim 1 further comprising "***means for updating the local authenticating means in response to a reply from the server***" (column 3 lines 27-32), wherein the local database is updated with the revocation information.

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Henry discloses:

The device recited in claim 2 further comprising "***means for updating the local authenticating means in response to a reply from the server***" (column 3 lines 27-32), wherein the local database is updated with the revocation information.

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Henry discloses:

The device recited in claim 3 further comprising "***means for updating the local authenticating means in response to a reply from the server***" (column 3 lines 27-32), wherein the local database is updated with the revocation information.

Regarding claim 7, Henry discloses:

A computer security method, comprising the step of:

"***locally-authenticating a user of the device***" (column 2 lines 12-39, column 3 lines 1-9, column 4 lines 3-24), wherein an access point receives an authentication

credential from a network device (secure computer device) and can locally authenticate the user;

"***providing granting previously authorized access to the device if the user is locally authenticated***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***generating a remote authentication request after a successful local authentication of the user***" (column 3 lines 6-9, column 4 lines 27-30), wherein after the local authentication of the user, the access point forwards the submitted credentials to a remote AAA server, which then performs the entire authentication process;

"***granting access to new activities and control parameters on the computer device if remote authentication is successful***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***unless the authorized activity is not completed, wherein the new activity is denied"*** wherein the mobile host encrypts and signs packets before sending the packets to the network (column 4 lines 45-50); and

"***storing identification data from a subsequent user while a previous user's activity is being completed***" wherein the queue where authentication requests are kept until the home AAA can process it (column 1 lines 59-63) holds authentication requests waiting for processing is interpreted as the storing the identification information while a previous user's activity is being completed

Regarding claim 13, Henry discloses:

A computer readable medium, comprising:

"***logic for locally-authenticating a user of the device***" (column 2 lines 12-39, column 3 lines 1-9, column 4 lines 3-24), wherein an access point receives an authentication credential from a network device (secure computer device) and can locally authenticate the user;

"***logic configured to grant previously authorized access to the device if the user is locally authenticated***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***logic for generating an authentication request after a successful local authentication of the user***" (column 3 lines 6-9, column 4 lines 27-30), wherein after the local authentication of the user, the access point forwards the submitted credentials to a remote AAA server, which then performs the entire authentication process;

"***logic configured to grant access to new activities and control parameters on the computer device if remote authentication is successful***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***unless the authorized activity is not completed, wherein the new activity is denied"*** wherein the mobile host encrypts and signs packets before sending the packets to the network (column 4 lines 45-50); and

"***storing identification data from a subsequent user while a previous user's activity is being completed***" wherein the queue where authentication requests are kept until the home AAA can process it (column 1 lines 59-63) holds authentication requests waiting for processing is interpreted as the storing the identification information while a previous user's activity is being completed.

6. Claims 8 – 12 are method claims analogous to the apparatus claims 1-6 rejected above, and therefore, are rejected following the same reasoning.

7. Claims 14 – 18 are computer-readable medium claims analogous to the apparatus claims 1-6 rejected above, and therefore, are rejected following the same reasoning.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Henry et al. (U.S. Patent No. 6,856,800) in view of Hosein et al. (U.S. Patent No. 6,430,694).

Regarding claim 19, Henry discloses:

"***a client having a client database for locally-authenticating a user***" (column 2 lines 12-39, column 3 lines 1-9, column 4 lines 3-24), wherein an access point receives an authentication credential from a network device (secure computer device) and can locally authenticate the user;

"***an authentication device that grants previously authorized non-controlling access if the user is locally authenticated***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***a server, in communication with the client, having a server database for remotely-authenticating the use in response to a request from the client after a successful local authentication***" (column 3 lines 6-9, column 4 lines 27-30), wherein after the local authentication of the user, the access point forwards the submitted credentials to a remote AAA server, which then performs the entire authentication process;

"***wherein the authentication device grants access to new activities and control parameters on the computer device if remote authentication is successful***" (Figure 4 item 404, column 3 lines 5-33), wherein the restricted temporary access is restricted in terms of limited valid time span, until a remote authentication is sent and can give full access;

"***unless the authorized activity is not completed, wherein the new activity is denied"*** wherein the mobile host encrypts and signs packets before sending the packets to the network (column 4 lines 45-50);

"***storing identification data from a subsequent user while a previous user's activity is being completed***" wherein the queue where authentication requests are kept until the home AAA can process it (column 1 lines 59-63) holds authentication requests waiting for processing is interpreted as the storing the identification information while a previous user's activity is being completed; and

"***means for updating the client database according to the results of the local and remote authentication***" (column 3 lines 27-32), wherein the local database is updated with the revocation information.

Henry does not explicitly disclose "***means for limiting a number of times that a particular client database and/or record in any, or all, of the client databases will be updated during any period of time and/or total number of updates***". However, Hosein discloses a database system, which is modified to include the ability to limit the number of data updates, which may be outstanding to the plurality of distributed databases during any particular period of time (column 2 lines 59-67). Henry and Hosein are analogous arts in that both utilize database systems. Hosein uses a modified database system, which can be implemented on any database to limit the number of data updates, which may be outstanding to the plurality of distributed databases during any particular period of time. This would have been obvious to modify

the database system of Henry to limit the number of updates in order to avoid the possibility of having databases not being synchronized. This would be disadvantageous in the system of Henry, because it would be beneficial to have all the local authentication clients (access points) to be synchronized with each other, so that a user that is being authenticated at one access point would receive the same authentication at another access point at approximately the same time (column 2 lines 43-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the database system of Henry to include the maximum number of outstanding updates, so that the local authentication databases of the local authenticating clients would be synchronized.

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Henry discloses:

The secure computer system recited in claim 19, further comprising:

"***means for authorizing a user in response to a successful local authentication***" (column 3 lines 1-9), wherein the access point can locally authenticate a user and then grant temporary access to the user immediately after the successful completion of the local authentication process; and

"***means for withdrawing the authorization in response to an unsuccessful remote authentication***" (column 3 lines 7-9, column 5 lines 4-17), wherein the remote server determines if the credentials are valid, and if the credentials are determined to be

invalid, a message is sent to the access point which terminates the user's temporary access.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
08/16/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

8/16/06